

Annual 47 C>F>R> 64.2009 (e) CPNI Certification for 2011

EB Docket 06-36

Date Filed: March 1, 2012

Name of Company: iFiber Communications Corporation

Form 499 Filer ID: 826772

Name of Signatory: W. Kelly Ryan

Title of Signatory: CEO

I, W. Kelly Ryan, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules.

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commissions' rules.

The company has not taken any actions against data brokers in the past year.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI.

Signed: \_\_\_\_\_



W. Kelly Ryan

CEO

iFiber Communications Corporation

135 Basin ST SW

Ephrata, WA 98823



*SAMPLE - All employees are required to  
read and sign upon hire*

## **CPNI Disclosure Safeguards**

**Corporate Policy:** It is the policy of iFIBER Communications Inc, (iFIBER) to comply with the FCC regulations, 47 C.F.R. § 64.2009(e). All iFIBER employees are required to follow the policies and procedures specified in this manual.

**Customer proprietary network information (CPNI) defined:** is the data collected by telecommunications corporations about a consumer's telephone calls. It includes the time, date, duration and destination number of each call, the type of network a consumer subscribes to, and any other information that appears on the consumer's telephone bill.

**Access to call records:** To protect against pretexting, (the practice of obtaining personal information under false pretenses), iFIBER Communications does not release call detail information during a customer-initiated call unless (1) The caller provides the account password (2) We call the customer back at the telephone number of record (3) We send the call records to the address of record (postal or electronic), or (4) We provide the call records at our retail location upon proof of valid photo ID matching the customer's account information.

**Online account access to any CPNI:** Online access to account information, including call detail information, requires that authentication be permitted only through the use of non-life-history-related passwords that each customer is instructed to create.

**Customer notification of account changes:** To alert customers to possible theft of CPNI, iFIBER provides notification whenever a password, backup authentication data, online account or address of record is created or changed. Notification is accomplished by voicemail, or e-mail, but must be sent to the telephone number or e-mail address of record and must not reveal the changed information.

**Business customer exception:** iFIBER does negotiate other authentication regimes for business customers, provided that (1) the customer has a dedicated account representative and (2) the negotiated service contract specifically addresses CPNI.

**CPNI for Marketing:** iFIBER does not use CPNI for marketing purposes.

### **Notification of Breaches**

**"Breach" defined:** A breach occurs when a person without authorization or one who is exceeding authorization has intentionally gained access to, used or disclosed CPNI.

**Notification to Supervisor:** Any complaints received concerning the unauthorized release of CPNI must be reported immediately to your direct supervisor.

**Notification to USSS and FBI:** iFIBER will notify the US Secret Service and FBI as soon as possible after reasonable determination of a breach, and in no event later than seven business days.

The FCC will maintain a link on its website to a central reporting facility at <http://www.fcc.gov/eb/CPNI>.

**Notification to customers and public:** iFIBER will not notify a customer, or make other public disclosure until seven business days after the USSS and FBI are informed, unless iFIBER believes there is an extraordinarily urgent need to notify customers sooner. iFIBER will cooperate with the relevant investigating agency prior to making any such early notification.

**Recordkeeping:** iFIBER will keep records of all breaches, notifications to the USSS and FBI, and notifications to customers, for at least two years. The records must include (if available) dates of discovery and notification, a detailed description of the CPNI at issue and the circumstances of the breach.

**Annual CPNI Certification:** An annual filing with the FCC will be made which includes an explanation of any actions taken against data brokers and a summary of all consumer complaints received regarding unauthorized release of CPNI.

**Improper use of CPNI:** Any improper use or release of CPNI by an iFIBER employee will result in disciplinary action in accordance with the established company policy as set forth in the employee manual, which may result in termination of employment.

#### Employee Verification

I have reviewed the iFIBER CPNI Disclosure Safeguard Manual and agree to comply with the procedures set forth herein.

Date: \_\_\_\_\_

Name: \_\_\_\_\_

Signature: \_\_\_\_\_

ⓧ All employees are  
required to read  
& Sign.